What I Claim Is:

~~Patent Claims~~

1

1. A method for generating asymmetrical cryptokeys at the user's location, in which keys are generated, personalized, and certified at a central, particularly secure location, (Trust Center), or, in cooperation using secure transmission between the user and this Trust Center, at the location of the user,

characterized in that

a. first, the user is provided by the Trust Center with a previously generated, personalized, and certified signature key pair (PS, ÖS), and also components for producing one or more encryption key pairs (GEK),

b. thereupon, a further user's-own encryption key pair having a public (ÖVS) and a secret part (PVS) is produced by the user, and the public part (ÖVS) is marked using the assigned secret part (PS) of the signature key and the result is transmitted to the Trust Center,

c. thereupon, the unequivocal assignment to the user is checked by the Trust Center using the certified public part (ÖS) of the signature key pair,

d. after a successful check of the assignment, a new certificate is produced by the Trust Center using at least a public part of the signature key pair (ÖS) or of the encryption key pair (ÖVS) of the user, and finally

e. this certificate, encrypted using the public part of the encryption key pair (ÖVS) of the user, is transmitted by the Trust Center to the user.

2. The method for generating asymmetrical cryptokeys at the user's location as recited in Claim 1, characterized in that the user, in method step a., is additionally provided with components (GDSK) for producing one or more signature key pairs, which, in method step b., are also produced by the user, and that the public part (ÖS2) of this self-generated signature key pair is marked by the user, in addition or simultaneously, using the secret part of the signature key pair (PS) received from the Trust Center.

3. The method for generating asymmetrical cryptokeys at the user's location as recited in Claim 1 and 2,

characterized in that a user (AW1) desiring no communication whatsoever with a Trust Center, in every bilateral communication with another user (AW2), first marks and makes available to the latter the public part of his self-generated key pair (ÖVS or ÖS2) using the secret part of the key pair (PS) previously relinquished, personalized, and certified by the Trust Center, whereupon the correct assignment of this information regarding the public part (ÖVS or ÖS2) of the key pair self-generated by the sending user (AW1) is checked by the receiving user (AW2) by verifying the signature, and the genuineness and validity of the certificate in the Trust Center underlying this signature can be checked.

A00 A47